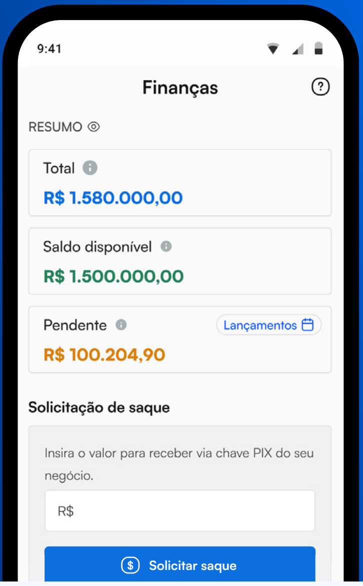
SHIELD | Kirvano

Case Study

Kirvano Partners SHIELD To Eliminate Fraud and Drive Revenue Growth for Digital Creators



9:41

Finanças

RESUMO

Total
R$ 1.580.000,00

Saldo disponível
R$ 1.500.000,00

Pendente — Lançamentos
R$ 100.204,90

Solicitação de saque

Insira o valor para receber via chave PIX do seu negócio.

R$

> “With SHIELD’s Device Intelligence, we’re able to accurately distinguish genuine customers and fraudsters. Our partnership with SHIELD is key to ensuring security and driving business growth for the digital content creators who rely on our platform.”
>
> **Lorram Félix**
> CEO, Kirvano

Key Takeaways

99% increase in account takeover detection

Ensured revenue growth for content creators by eliminating fraud

Detected payment fraud signals in real-time, preventing financial losses

Kirvano and Its Path to Securing a Trustworthy Platform for Users

Kirvano’s mission is to empower digital content creators and online entrepreneurs by providing a secure and efficient platform that facilitates the creation, sale, and promotion of their digital products and services.

Providing a seamless experience for content creators using the ecosystem to sell and promote their products and services is of utmost importance for Kirvano. However, they were also aware that their platform could fall prey to bad actors, who can undermine the growth of creators by conducting payment fraud and taking over accounts, jeopardizing trust on the platform.

To address this critical issue, Kirvano chose to partner with SHIELD, the device-first fraud intelligence platform. SHIELD’s technology detects and eliminates fraudulent activity in real time ensuring a trustworthy

Customer Profile

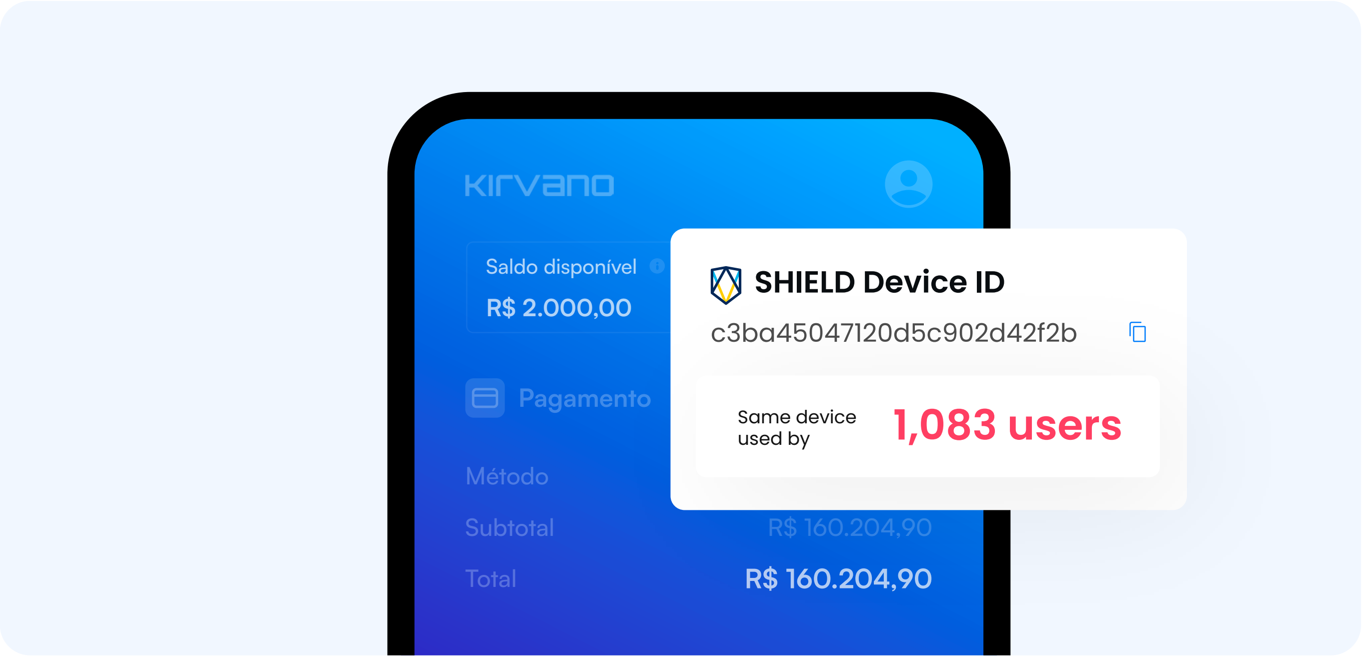
Founded in 2022, Kirvano is a Brazilian startup that offers payment and sales management solutions for digital content creators and online entrepreneurs. The platform stands out for its ease of use, competitive rates, and customer focus.

Industry

Payment Solution for Digital Products and Services

Region

LATAM



Kirvano

Saldo disponível
R$ 2.000,00

Pagamento

Método

Subtotal R$ 160.204,90

Total R$ 160.204,90

SHIELD Device ID
c3ba45047120d5c902d42f2b

Same device used by 1,083 users

environment for Kirvano's digital content creators. This partnership not only protects the platform but also drives growth for businesses relying on Kirvano, reinforcing its mission to empower and support the success of digital entrepreneurs.

From ATO to Payment Fraud: The Threats Affecting Kirvano

There are several methods that fraudsters use to target platforms similar to Kirvano.

Account takeovers (ATO) are a common tactic that can affect both content creators' accounts and users' accounts (those who purchase the products/services offered by digital content creators). By employing techniques such as social engineering and credential stuffing, fraudsters gain access to legitimate accounts and can:

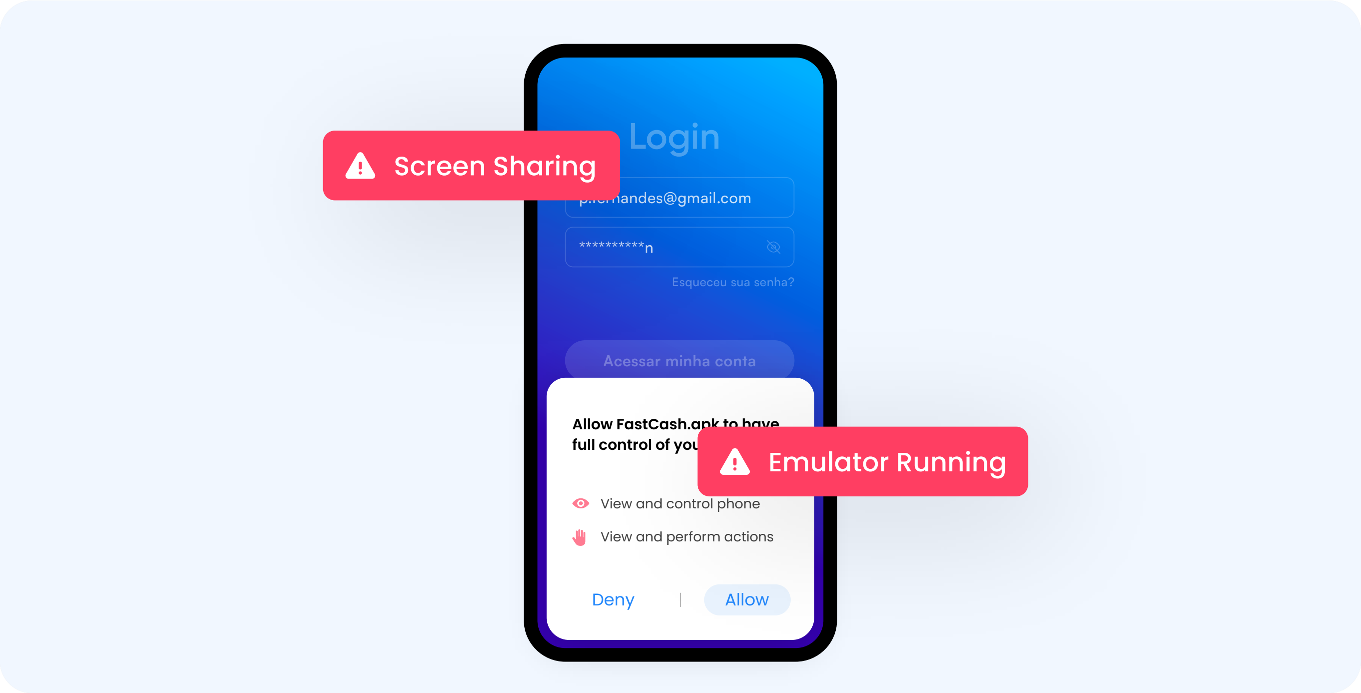
- **Users' Accounts:** Access sensitive payment information stored within the account, such as credit card numbers, which can then be used for fraudulent activities like payment fraud or even sold on the dark web.
- **Content Creators' Accounts:** Change personal information, transfer the available balance from the digital content creator's account to their own bank account, and even delete the creator's content, leading to financial and time losses.

Payment fraud is another significant threat in this industry. Fraudsters conduct unauthorized transactions using fake accounts combined with sensitive information, such as credit card numbers, obtained through ATO attacks, stolen credit cards, or information from the dark web. This results not only in high chargeback rates but also gives content creators an illusion of higher sales, eroding trust in the platform.

To stop ATO and payment fraud attempts, Kirvano's team relies on **SHIELD Device ID**, which persistently identifies every physical device on the platform, eliminating fraud at its root. It precisely identifies:

- **Multiple Accounts Accessed From a Single Device:** Usually, all the taken-over accounts are associated with a single device being operated by the fraudster;
- **Unfamiliar Devices:** The sudden appearance of unrecognized devices logged into the same account or multiple logins from different locations in a short time;
- **Multiple IP Address or Geolocations:** If there were multiple login attempts on a single account from different geographies.

These are all signs of account takeover attempts that SHIELD's technology can detect in real time to prevent this form of fraud.



Moreover, **SHIELD's Fraud Intelligence** profiles each device session, returning real-time risk signals to provide a comprehensive picture of user activity in the platform. It can pinpoint the precise moment when a legitimate user shows signs of fraudulent behavior. This feature allows detection of devices that trigger malicious tools such as **emulators** and **screen sharing**, often employed in ATO attacks and payment fraud.

Building a Trustworthy Platform with SHIELD

Kirvano has taken a proactive stance against the ever-evolving landscape of fraud by teaming up with SHIELD and implementing the Device-First Fraud Intelligence platform. Powered by cutting-edge device fingerprinting and the latest in AI & machine learning algorithms, our solution equips Kirvano with real-time device intelligence. This empowers Kirvano's team to swiftly detect and mitigate threats, safeguarding both users and digital content creators alike.

"With SHIELD's Device Intelligence, we're able to accurately distinguish genuine customers and fraudsters. Our partnership with SHIELD is key to ensuring security and driving business growth for the digital content creators who rely on our platform", added Lorram Félix, CEO at Kirvano.

SHIELD is a device-first fraud intelligence platform that helps digital businesses worldwide eliminate fake accounts and stop all fraudulent activity.

Powered by SHIELD AI, we identify the root of fraud with the global standard for device identification (SHIELD Device ID) and actionable fraud intelligence, empowering businesses to stay ahead of new and unknown fraud threats.

We are trusted by global unicorns like inDrive, Alibaba, Swiggy, Meesho, TrueMoney, and more. With offices in San Francisco, London, Berlin, Jakarta, Bengaluru, Beijing, and Singapore, we are rapidly achieving our mission - eliminating unfairness to enable trust for the world.

For more information, visit **shield.com**.

/shieldfraud

/shieldfraud

/company/shield

shield.com

ISO 27001 Certified

GDPR

AICPA SOC 2

PCI DSS COMPLIANT